1/3/1
DIALOG(R)File 351:Derwent WPI

015258456 **Image available**
WPI Acc No: 2003-319385/ **200331**
XRPX Acc No: N03-254626

Domain name system server data alteration system, has certificate server that deletes information related to computer from DNS server, after internet connection is disconnected

Patent Assignee: IV NETWORK KK (IVNE-N); NTT SOFTWARE KK (NITE)
Number of Countries: 001 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2003018183	A	20030117	JP 2001199606	A	20010629	200331	B
JP 3613392	B2	20050126	JP 2001199606	A	20010629	200510	

Priority Applications (No Type Date): JP 2001199606 A 20010629
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2003018183	A		7	H04L-012/56	
JP 3613392	B2		9	H04L-012/56	Previous Publ. patent JP 2003018183

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-018183
(43)Date of publication of application : 17.01.2003

(51)Int.Cl. H04L 12/56

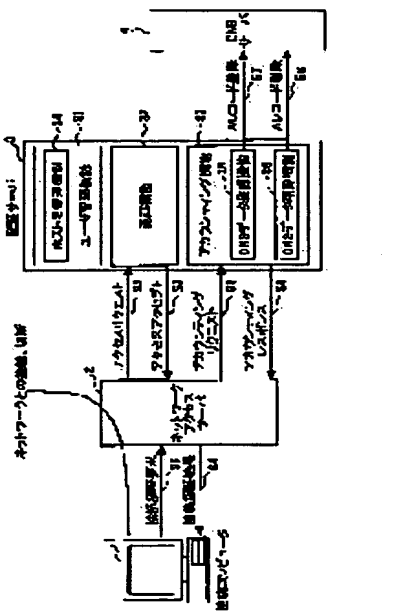
(21)Application number : 2001-199606
(22)Date of filing : 29.06.2001

(71)Applicant : IVYNETWORK CO LTD
NTT SOFTWARE CORP
(72)Inventor : MORIZAKI MASATO
MIZUNUMA SHINJI
SHINODA AKIRA

(54) DNS SEVER DATA CHANGING SYSTEM AND AUTHENTICATION SERVER

(57)Abstract:
PROBLEM TO BE SOLVED: To surely register/delete data in a dynamic DNS server, at using of an emergency connection service to the Internet.
SOLUTION: An authentication sever checks prescribed information in a message related with charging received from a network access server, and when the prescribed information indicates that a user computer is starting its connection to the Internet, registers data related with the computer in a DNS server; and when the prescribed information indicates that the user computer has ended the connection to the Internet, the server deletes the data related with the computer from the DNS server.

本発明の実施例におけるインターネット接続システムの構成を示す図



LEGAL STATUS

[Date of request for examination]	29.06.2001
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3613392
[Date of registration]	05.11.2004
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－18183
（P2003－18183A）
(43)公開日　平成15年１月17日(2003.1.17)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　12/56	Ｂ　５Ｋ０３０

審査請求　有　　請求項の数５　ＯＬ　（全　７　頁）

(21)出願番号　特願2001－199606(P2001－199606)

(22)出願日　平成13年６月29日(2001.6.29)

(71)出願人　500056633
株式会社アイヴィネットワーク
神奈川県横浜市西区南浅間町14－４

(71)出願人　000102717
エヌ・ティ・ティ・ソフトウェア株式会社
神奈川県横浜市中区山下町223番１

(72)発明者　森▲崎▼　正人
神奈川県横浜市西区南浅間町14－４　株式会社アイヴィネットワーク内

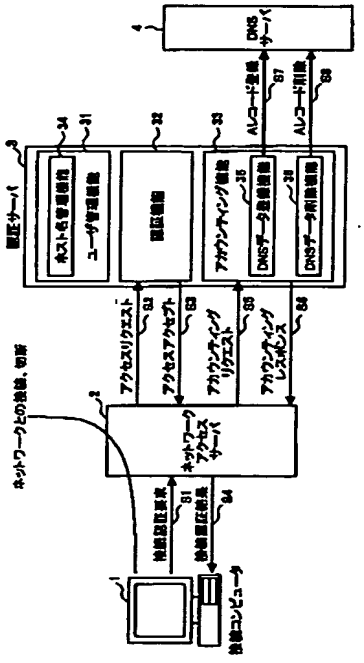
(74)代理人　100070150
弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】　ＤＮＳサーバデータ変更システム及び認証サーバ

(57)【要約】
【課題】　インターネットへの非常時接続サービスを利用する場合において、ダイナミックＤＮＳサーバへのデータ登録／削除を確実に行なう。
【解決手段】　認証サーバが、ネットワークアクセスサーバから受信した課金に関するメッセージの中の所定の情報を調べ、該所定の情報が、ユーザコンピュータがインターネットへの接続を開始する旨を表す場合にはＤＮＳサーバに前記コンピュータに関するデータを登録し、該所定の情報が、ユーザコンピュータがインターネットと接続終了した旨を表す場合にはＤＮＳサーバから前記コンピュータに関するデータを削除する。

本発明の実施例におけるインターネット接続システムの構成を示す図



1

【特許請求の範囲】

【請求項１】　コンピュータがインターネットと接続又は切断する際にＤＮＳサーバのデータを変更するシステムであって、

前記コンピュータからインターネット接続のための接続要求を受け付けるネットワークアクセスサーバと、

該接続要求を受け付けたネットワークアクセスサーバからの要求に応じて前記コンピュータの認証を行う認証サーバとを有し、

認証サーバは、ネットワークアクセスサーバから受信した課金に関するメッセージの中の所定の情報を調べ、

該所定の情報が、前記コンピュータがインターネットへの接続を開始する旨を表す場合にはＤＮＳサーバに前記コンピュータに関するデータを登録し、該所定の情報が、前記コンピュータがインターネットと接続終了した旨を表す場合にはＤＮＳサーバから前記コンピュータに関するデータを削除することを特徴とするシステム。

【請求項２】　前記認証サーバは、

前記所定の情報が、前記コンピュータがインターネットへの接続を開始する旨を表す場合に、前記メッセージから前記コンピュータのユーザ名とＩＰアドレス情報とを取得し、該ユーザ名に対応したホスト名を取得し、該ＩＰアドレス情報と該ホスト名とを前記ＤＮＳサーバに登録し、

該所定の情報が、前記コンピュータがインターネットと接続終了した旨を表す場合に、前記メッセージから前記コンピュータのユーザ名を取得し、該ユーザ名に対応したホスト名を取得し、該ホスト名に対応するデータを前記ＤＮＳサーバから削除する請求項１に記載のシステム。

【請求項３】　前記課金に関するメッセージは、Ｒａｄｉｕｓプロトコルにおけるアカウンティングリクエストメッセージであり、前記所定の情報はアカウンティングリクエストメッセージの中のステータスタイプである請求項１又は２に記載のシステム。

【請求項４】　コンピュータがインターネットと接続又は切断する際にＤＮＳサーバのデータを変更するシステムにおいてコンピュータの認証を行う認証サーバであって、

ネットワークアクセスサーバから受信した課金に関するメッセージの中の所定の情報を調べる手段と、

該所定の情報が、前記コンピュータがインターネットへの接続を開始する旨を表す場合にはＤＮＳサーバに前記コンピュータに関するデータを登録する手段と、

該所定の情報が、前記コンピュータがインターネットと接続終了した旨を表す場合にはＤＮＳサーバから前記コンピュータに関するデータを削除する手段とを有することを特徴とする認証サーバ。

【請求項５】　前記登録する手段は、

前記所定の情報が、前記コンピュータがインターネットへの接続を開始する旨を表す場合に、前記メッセージから前記コンピュータのユーザ名とＩＰアドレス情報とを取得し、該ユーザ名に対応したホスト名を取得し、該ＩＰアドレス情報と該ホスト名とを前記ＤＮＳサーバに登録する手段を有し、

前記削除する手段は、

該所定の情報が、前記コンピュータがインターネットと接続終了した旨を表す場合に、前記メッセージから前記コンピュータのユーザ名を取得し、該ユーザ名に対応したホスト名を取得し、該ホスト名に対応するデータを前記ＤＮＳサーバから削除する手段を有する請求項４に記載の認証サーバ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネット上のドメインネームシステム（ＤＮＳ）のデータを変更する技術に関する。

【０００２】

【従来の技術】インターネット上で情報発信を行う場合、コンピュータを情報発信サーバとして設置し、外部からのアクセス用のアドレスとしてＩＰアドレスそのものではなくＵＲＬを公開する。このＵＲＬは、ホスト名とドメイン名とサーバ上のファイルの位置から構成される。

【０００３】従って、サーバにアクセスする際には、ホスト名とドメイン名の組み合わせからＩＰアドレスを取得する必要がある。そのために、ホスト名とドメイン名の組み合わせをＩＰアドレスに変換するサービスとしてドメインネームシステム（ＤＮＳ）があり、ＲＦＣ１０３５で規定されている。

【０００４】すなわち、公開されたＵＲＬにより情報発信サーバへのアクセスを行う場合、ホスト名とドメイン名の組み合わせをＤＮＳに問い合わせてＩＰアドレスに変換し、変換されたＩＰアドレスにより情報発信サーバへ接続することとなる。

【０００５】さて、情報発信サーバをインターネットに接続する場合、インターネットサービスプロバイダー（ＩＳＰ）の常時接続サービスを用いる方法のほか、ダイアルアップ相当の非常時接続サービスを用いる方法がある。常時接続サービスではＩＰアドレスが情報発信サーバに固定的に付与されるが、ダイアルアップ相当の非常時接続サービスではインターネットに接続する都度付与されるＩＰアドレスが変更される。

【０００６】従って、ダイアルアップ相当の非常時接続サービスを使用して情報発信サーバを設置した場合、ＩＳＰから付与されるＩＰアドレスが変更される度、すなわち、情報発信サーバがインターネットに接続する度に、ＤＮＳサーバにおけるホスト名とドメイン名との組み合わせとＩＰアドレスの射影を変更する必要が生じる。

【０００７】従来技術では、ホストの追加、変更等があった場合のＤＮＳサーバのデータ更新は、データファイルを手動で直接編集し更新するか、ＲＦＣ２１３６で規定されているＤＮＳのデータに対する動的変更方法によりＤＮＳサーバ（ダイナミックＤＮＳサーバ）へアクセスするツールを用いて手動で行なっている。

【０００８】ＲＦＣ２１３６で規定されている方法によりＤＮＳデータのＡレコード更新を行なう場合、ユーザが手動で接続時にＤＮＳデータの登録、切断前にＤＮＳデータの削除を行なうことになる。この場合、接続時は外部からのアクセスを確保するため登録を行なうが、データ削除は、接続コンピュータの不意な停止、接続回線の不意な切断、もしくは削除忘れなどにより、必ずしも行なわれるとは限らない。

【０００９】

【発明が解決しようとする課題】上述したように、非常時接続サービスを利用する場合におけるＤＮＳサーバに対するデータの登録／削除を手動で行わなければならない上、削除が確実に行なわれないという問題がある。

【００１０】本発明は、上記に鑑みてなされたもので、インターネットへの非常時接続サービスを利用する場合において、ＤＮＳサーバへのデータ登録／削除を自動的に確実に行なうことを可能にする技術を提供することを目的とする。

【００１１】

【課題を解決するための手段】上記目的を達成するため、本発明は次のように構成することができる。

【００１２】請求項１に記載の発明は、コンピュータがインターネットと接続又は切断する際にＤＮＳサーバのデータを変更するシステムであって、前記コンピュータからインターネット接続のための接続要求を受け付けるネットワークアクセスサーバと、該接続要求を受け付けたネットワークアクセスサーバからの要求に応じて前記コンピュータの認証を行う認証サーバとを有し、認証サーバは、ネットワークアクセスサーバから受信した課金に関するメッセージの中の所定の情報を調べ、該所定の情報が、前記コンピュータがインターネットへの接続を開始する旨を表す場合にはＤＮＳサーバに前記コンピュータに関するデータを登録し、該所定の情報が、前記コンピュータがインターネットと接続終了した旨を表す場合にはＤＮＳサーバから前記コンピュータに関するデータを削除する。

【００１３】請求項２に記載の発明は、請求項１の記載において、前記認証サーバは、前記所定の情報が、前記コンピュータがインターネットへの接続を開始する旨を表す場合に、前記メッセージから前記コンピュータのユーザ名とＩＰアドレス情報とを取得し、該ユーザ名に対応したホスト名を取得し、該ＩＰアドレス情報と該ホスト名とを前記ＤＮＳサーバに登録し、該所定の情報が、前記コンピュータがインターネットと接続終了した旨を表す場合に、前記メッセージから前記コンピュータのユーザ名を取得し、該ユーザ名に対応したホスト名を取得し、該ホスト名に対応するデータを前記ＤＮＳサーバから削除する。

【００１４】請求項３に記載の発明は、請求項１又は２の記載において、前記課金に関するメッセージは、Ｒａｄｉｕｓプロトコルにおけるアカウンティングリクエストメッセージであり、前記所定の情報はアカウンティングリクエストメッセージの中のステータスタイプであるとする。

【００１５】請求項４、５に記載の発明は、上記システムでの使用に適した認証サーバである。

【００１６】本発明によれば、認証サーバが、ネットワークアクセスサーバから受信した課金に関するメッセージの種別に応じてＤＮＳサーバのデータ登録／削除処理をすることにより、ユーザコンピュータの通信の接続／切断とＤＮＳサーバのデータ登録／削除処理を連動させることが可能となる。従って、従来のような手動によるＤＮＳデータ登録を行う必要がなくなり、また、ＤＮＳサーバのデータ削除を確実に行うことが可能となる。

【００１７】

【発明の実施の形態】以下、図面を用いて本発明の実施例を説明する。

【００１８】図１は、本発明の実施例におけるインターネット接続システムの構成を示す図である。

【００１９】同図に示すインターネット接続システムは、接続コンピュータ１、ネットワークアクセスサーバ２、認証サーバ３、ＤＮＳサーバ４を有する。

【００２０】接続コンピュータ１は、インターネットサービスプロバイダの非常時接続サービスを利用してインターネットに接続する情報公開サーバ等であり、ネットワークアクセスサーバ２へ接続し、認証サーバ３による認証後にネットワークアクセスサーバ２を介してインターネットへアクセス可能となる。ネットワークアクセスサーバ２は、認証及びアカウンティングのためにＲａｄｉｕｓプロトコルによって認証サーバ３へアクセスする。ＤＮＳサーバ４は、ホスト名とドメイン名の組み合わせをＩＰアドレスに変換する機能を有する。

【００２１】認証サーバ３は、ユーザ管理機能３１、認証機能３２、アカウンティング機能３３を有し、本発明ではＤＮＳサーバ４のデータ更新を行う機能も有する。ユーザ管理機能３１は、ユーザ名、パスワードなどのユーザ情報を管理する機能であり、本発明ではホスト名管理機能３４を加えて、ユーザ毎に接続するコンピュータに対するホスト名を管理する。認証機能３２は、認証要求を受信した場合、ユーザ管理機能３１から該当するユーザの情報を取得し、認証を行なう機能である。アカウンティング機能３３は、アカウンティングメッセージを受信した場合にアカウンティング情報をログに書き出す機能である。

【００２２】本発明では、アカウンティング機能３３にＤＮＳデータ登録機能３５とＤＮＳデータ削除機能３６を追加し、ＤＮＳサーバ４のデータに対して操作を行なう。

【００２３】なお、認証サーバ３で用いられるＲａｄｉｕｓプロトコルは、インターネット接続時のユーザアクセス認証、アカウンティング等によく用いられているものであり、認証に関するものはＲＦＣ２８６５、アカウンティングに関するものはＲＦＣ２８６６で規定されている。

【００２４】上記の各サーバは、ＣＰＵ、メモリ、ハードディスク、入出力装置、通信制御装置等を有するコンピュータに各サーバの処理手順を実行するためのプログラムを搭載することによって実現できる。

【００２５】次に、図１を参照して、本実施例におけるインターネット接続システムの動作について説明する。なお、ＤＮＳサーバのデータ変更を除き、以下の手順はＲａｄｉｕｓプロトコルに基づく手順である。

【００２６】接続コンピュータ１からインターネット接続しようとする場合、接続コンピュータ１からネットワークアクセスサーバ２へ接続認証要求を出す（ステップ１）。その要求を受けたネットワークアクセスサーバ２は、認証のために認証サーバ３へＲａｄｉｕｓプロトコルにより通信を行なう。すなわち、アクセスリクエストメッセージを認証サーバ３に送信する（ステップ２）。認証サーバ３により認証がなされたときには、認証サーバ３はアクセスアクセプトメッセージをネットワークサーバ２に送信する（ステップ３）。これにより、接続認証結果が接続コンピュータ１に送られ（ステップ４）、接続コンピュータ１はインターネットに接続できることとなる。

【００２７】また、認証が成功した場合、ネットワークアクセスサーバ２は、アカウンティングを行うためのアカウンティングリクエストメッセージを認証サーバ３へ送信し（ステップ５）、認証サーバ３はアカウンティングレスポンスメッセージを返す（ステップ６）。

【００２８】インターネットへの接続時のアカウンティングリクエストメッセージにより認証サーバ３に通信開始であることが記録される。また、接続コンピュータ１とネットワークアクセスサーバ２間の通信が、通信終了も含めなんらかの理由のために切断された場合、ネットワークアクセスサーバ２から認証サーバ３へ通信終了を知らせるためのアカウンティングリクエストメッセージが送信され、これにより認証サーバ３に通信終了であることが記録される。

【００２９】本発明では、上記のアカウンティングリクエストメッセージを契機として認証サーバ３がＤＮＳサーバ４のデータ（Ａレコード）の登録や削除を行う（ステップ７、８）。この動作について図２の手順に従って詳細に説明する。

【００３０】図２はアカウンティング機能の処理シーケンスを示したものであり、点線内の部分が本発明におけるＤＮＳデータ登録機能３５及びＤＮＳデータ削除機能３６の動作である。

【００３１】まず、認証サーバ３がアカウンティングリクエストメッセージを受信すると、アカウンティングリクエストメッセージ内のステータスタイプをチェックする（ステップ１１）。

【００３２】図３にアカウンティングメッセージのフォーマットを示す。同図における属性の部分にステータスタイプが含まれる。また、コード（４又は５）によってアカウンティングリクエストかアカウンティングレスポンスかが識別される。

【００３３】アカウンティングリクエストメッセージ内のステータスタイプは、接続コンピュータ１がネットワークアクセスサーバ２に接続される場合には、スタート(Acct-Status-type=Start)となり、接続コンピュータ１がネットワークアクセスサーバ２から切断された場合には、ステータスタイプがストップ(Acct-Status-type=Stop)となる。図４にログファイルとして出力する属性の一例を示す（接続時の例）。

【００３４】次に、認証サーバ３は、上記のステータスタイプによって処理を振り分ける（図２のステップ１２）。

【００３５】ステータスタイプがスタートの場合には、アカウンティングリクエストメッセージからユーザ名とＩＰアドレス情報を取得し（ステップ１３）、ユーザ管理機能３１のホスト名管理機能３４からユーザ名に対応したホスト名を取得し（ステップ１４）、そのＩＰアドレス情報とホスト名をＡレコードとして、ＤＮＳサーバ４に登録する（ステップ１５）。

【００３６】ステータスタイプがストップの場合には、アカウンティングリクエストメッセージからユーザ名を取得し、ユーザ管理機能３１のホスト名管理機能３４からユーザ名に対応したホスト名を取得し（ステップ１６）、該ホスト名に対応するＡレコードを、ＤＮＳサーバ４から削除する（ステップ１７）。

【００３７】図５（ａ）に、通常のユーザ管理機能でのデータ構造を示し、図５（ｂ）に、本発明においてホスト名管理機能３４を追加するために上記データ構造に“ホスト名”を加えたユーザ管理機能３１のデータ構造を示す。このホスト名管理機能３４を用いることにより、図６（ａ）に示すＡレコード登録時に用いるデータ及び図６（ｂ）に示すＡレコード削除時に用いるデータを得ることが可能となる。

【００３８】図７にＤＮＳサーバ４におけるデータの記述例を示す。本発明によって、同図に示すホスト名を持つコンピュータがインターネットに接続されるときに当該ホスト名に対応するレコードが自動的に追加され、切断されるときに当該ホスト名に対応するレコードが自動

的に削除される。

【００３９】続いて、アカウンティングログの書き込みを行い（ステップ１８）、アカウンティングレスポンスメッセージをネットワークアクセスサーバに送信する（ステップ１９）。

【００４０】本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。例えば、上記の実施例ではＲａｄｉｕｓプロトコルを使用した場合を示したが、上記のアカウンティングメッセージに相当するメッセージを用いるプロトコルであれば、Ｒａｄｉｕｓプロトコル以外のプロトコルにも本発明を適用することが可能である。

【００４１】

【発明の効果】以上説明したように、本発明によれば、Ｒａｄｉｕｓプロトコルを使用した認証サーバが、アカウンティングリクエストメッセージのステータスタイプに従って、ＤＮＳサーバへのデータ登録／削除を行なうこととしたので、ユーザがコンピュータをインターネット接続／切断する際に手動でダイナミックＤＮＳサーバへデータを登録／削除する必要がなくなる。従って、インターネットサービスプロバイダは、利便性の高いインターネット非常時接続サービスを提供することが可能となる。

【００４２】また、ネットワークアクセスサーバからの回線接続状態に従ったダイナミックＤＮＳとの連動が可能となるため、接続回線の不意な切断や、接続したコンピュータの不意なダウンなどの場合も、回線切断状態として検知でき、ＤＮＳサーバに対して自動的にデータ削除処理を行なうことができ、不用意に使用しないデータが残存することを防止することが可能となる。

【００４３】

【図面の簡単な説明】

【図１】本発明の実施例におけるインターネット接続システムの構成を示す図である。

【図２】本発明の実施例におけるインターネット接続システムの動作を示すフローチャートである。

【図３】アカウンティングメッセージのフォーマットを示す図である。

【図４】ログファイルとして出力する属性の一例を示す図である（接続時の例）。

【図５】ユーザ管理機能におけるデータ構造を示す図である。

【図６】Ａレコード登録又は削除時に用いるデータを示す図である。

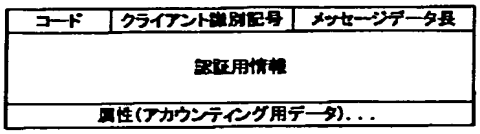
【図７】ＤＮＳサーバにおけるデータの記述例を示す図である。

【符号の説明】

１　接続コンピュータ
２　ネットワークアクセスサーバ
３　認証サーバ
４　ＤＮＳサーバ
３１　ユーザ管理機能
３２　認証機能
３３　アカウンティング機能
３４　ホスト名管理機能
３５　ＤＮＳデータ登録機能
３６　ＤＮＳデータ削除機能

【図３】

アカウンティングメッセージのフォーマットを示す図



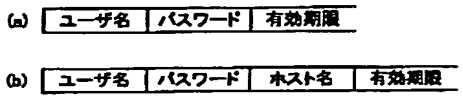
【図４】

ログファイルとして出力する属性の一例を示す図（接続時の例）

```
Mon Oct  4 11:54:14 1999
        User-Name = "user01@xxx.co.jp¥000"
        NAS-IP-Address = 157.X.XXX.XX
        NAS-Port = 2048
        NAS-Port-Type = Sync
        Acct-Status-Type = Start
        Acct-Delay-Time = 0
        Acct-Session-Id = "3074886938¥000"
        Acct-Authentic = RADIUS
        Ascend-Modem-PortNo = 2
        Ascend-Modem-SlotNo = 2
        Ascend-Modem-ShelfNo = 1
        Timestamp = 939005654
```

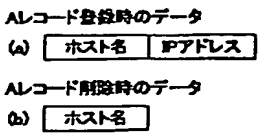
【図５】

ユーザ管理機能におけるデータ構造を示す図



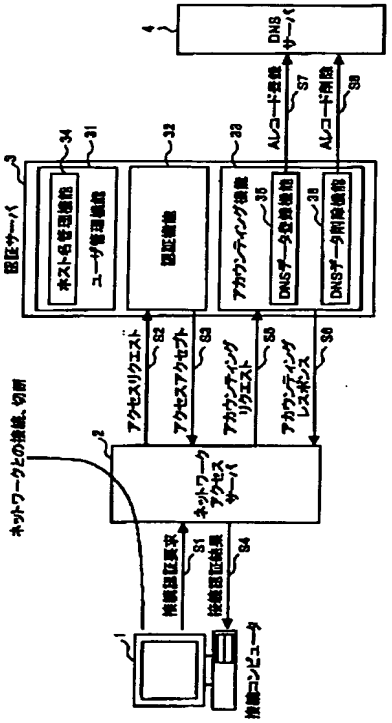
【図６】

Ａレコード登録又は削除時に用いるデータを示す図



【図１】

本発明の実施例におけるインターネット接続システムの構成を示す図



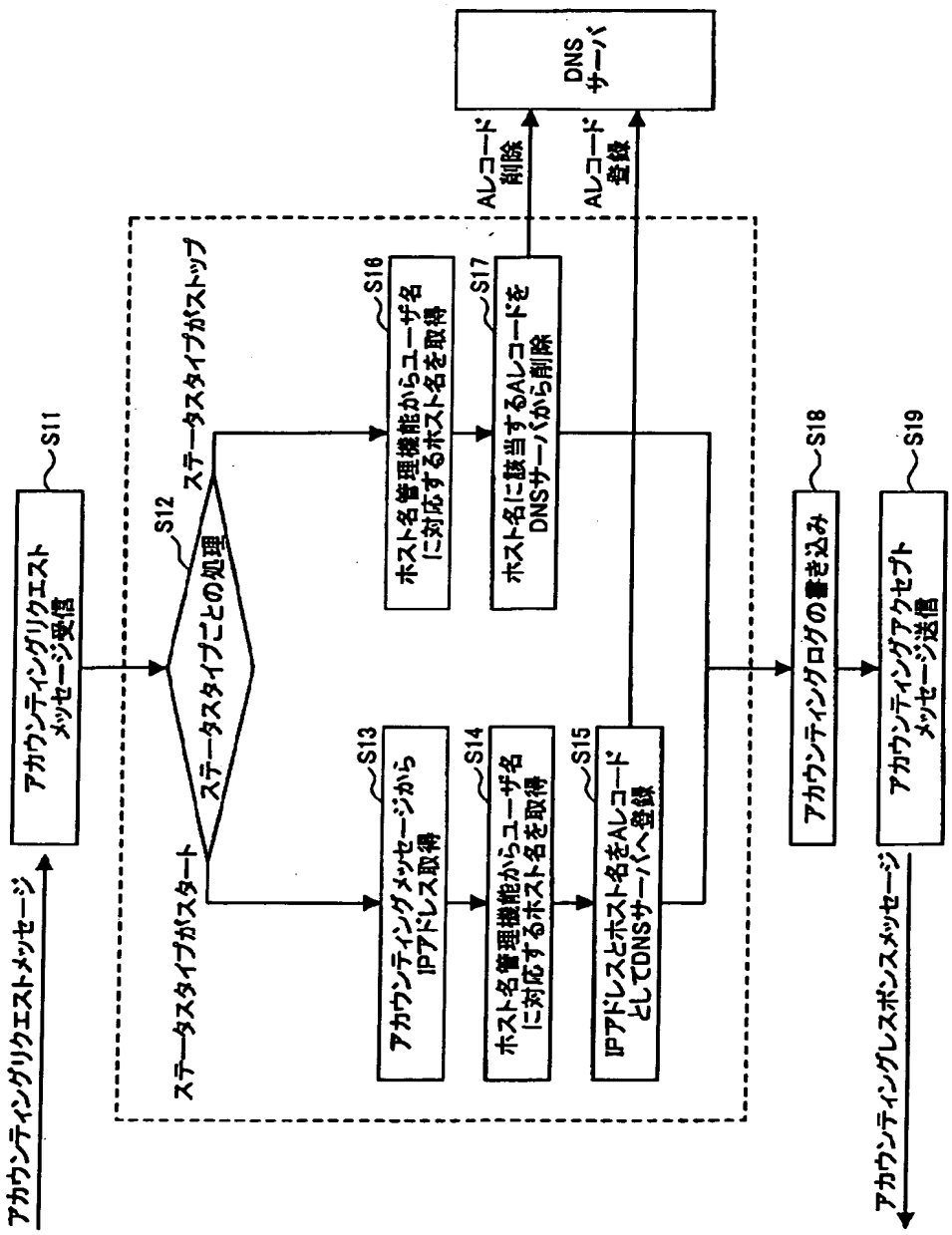
【図７】

ＤＮＳサーバにおけるデータ記述例を示す図

ホスト名			IPアドレス
↓			↓
yellow	IN	A	192.XXX.XXX.XXX
sonic	IN	A	192.XXX.XXX.XXX
hurricane	IN	A	192.XXX.XXX.XXX

【図２】

本発明の実施例におけるインターネット接続システムの動作を示すフローチャート



フロントページの続き

(72)発明者　水沼　信治
神奈川県横浜市西区南浅間町14－４　株式会社アイヴィネットワーク内

(72)発明者　篠田　晃
神奈川県横浜市中区山下町223番１　エヌ・ティ・ティ・ソフトウェア株式会社内

Ｆターム(参考)　5K030 GA15 HB08 KA05